

13.4.2007

CERT-FI

INFORMATIONSSÄKERHETSÖVERSIKT 1/2007

Under årets första kvartal fick CERT-FI veta om fler blockeringsattacker eller attackförsök än normalt. De mest nämnvärda attackerna riktade sig mot Internets namnservrar och mot webbtjänster för ett finländskt företag. Avvikande från vanliga fall var att attacken mot det finländska företaget skedde med ett självständigt fungerande skadligt program.

Det skickades en omfattande mängd skräppostmeddelanden med reklam för webbsidor som användes för att ta reda på nätbankskundernas användaridentifikationer och lösenord. En del av serverna som användes för nätfiske och domännamn som förde till serverna var aktiva för flera veckor. Alla befann sig i utländska nät. Fall där spionprogram har använts mot finländska servrar har än så länge varit sällsynta, men det finns vissa tecken på att situationen kan ändras.

Sårbarheter hittades i program som används i arbetsstationer och internet-routrar. Dessutom hittades sårbarheter i SCADA-system som används för processtyrning inom industrin. Sårbarheter publiceras också i fortsättningen i samband med kampanjer kring ett visst programvara eller operativsystem.

Blockeringsattack mot rotnamnservrar

Det skedde en blockeringsattack mot internets rotnamnservrar i början av februari. Attacken utfördes med hjälp av ett botnät, dvs. nätverk av angripna datorer. Attacken varade under ett dygn. Även om belastningen var stor, förblev inverkningarna små, och tio rotservrar bibehöll sin funktion. När funktion av tre logiska rotservrar hindrades, blev användarnas internetanvändning något långsammare.

Vid attacken upptäcktes också att några nationella domännamssystem var föremål för blockering. En del av störningarna berodde på att namntjänsterna för dessa toppdomäner producerades med samma system som internets rotnamntjänst.

Attackerna hade inte några inverknings på FI-domännamnets servicenivå, även om Kommunikationsverket och aktörer som tillhandahåller namnservrar höjde beredskapsnivån för en tid. Man beslöt att systemet som kontrollerar FI-namnservrarnas funktion tas i drift tidigare än planerat.

Öppna namnservrar som verktyg för blockeringsattacker

Eftersom domännamssystemet inte kontrollerar parternas autenticitet, är systemet utsatt för adressförfalskning. Om man missbrukar denna egenskap kan man få en sk. rekursiv resolver att fungera som förstärkare för attacken. Då styrs svaren till DNS-förfrågningar till den tredje part som är föremålet för attacken. Det blir en distribuerad blockeringsattack i föremålet, när stora mängder falska förfrågningar skickas till många namnservrar. I allmänhet är det svårt att få reda på den som orsakat trafiken även om många parter samarbetar aktivt.

CERT-FI fick den 9 februari 2007 veta om en mycket omfattande blockeringsattack som även utnyttjade finländska namnservrar. En motsvarande attack förekom den 28 februari 2007. Båda gånger tog Kommunikationsverket kontakt med aktörer som upprätthåller finländska servrar och uppmanade dem att ändra serverns inställningar så att något utnyttjande inte längre vore möjligt.

13.4.2007

CERT-FI

Blockeringsattack av typen fire and forget

Sedan juli 2006 har ett skadligt program Allaple spridit sig i informationsnäten. Programmets enda syfte är att hindra vissa webbtjänsters funktion. Intressant i fallet är att ett av föremålen befinner sig i ett finländskt nät.

För blockeringsattacker används vanligen fjärrstyrda nätverk, så kallade botnät. Nätmasken Allaple fungerar dock på ett annat sätt. Programmet enbart sprider sig och orsakar störande nättrafik till de adresser som angriparen har bestämt. Efter att programmet har släppts ut fungerar det helt självständigt, och det finns ingen kommando- eller styrförbindelse till det.

Att kommandoförbindelsen saknas betyder också att trafik som den spridande masken orsakar inte längre kan stoppas. Problemet avskaffas först när alla infekterade datorer har kopplats bort från nätet och programmet slutar sprida sig. Det är svårt att filtrera skadlig nättrafik som programmet orsakar därför att trafiken kommer från olika delar av världen och den ser likadan ut som förbindelserna för dem som har rätt att använda tjänsten.

Allaple har orsakat sina föremål stora svårigheter trots att teleoperatören har vidtagit massiva åtgärder för trafikfiltrering.

Blockeringsattacker mot e-postservrar

CERT-FI blev också informerad om blockeringsattacker mot finländska e-postservrar.

Det är möjligt att målsystemets prestation har prövats genom en sådan långvarig attack. Ett ökat antal förbindelser har betytt ökad belastning i servrarna men tjänsten har dock inte helt blockerats. Servern har belastats med en massa meddelanden till påhittade adresser.

I slutet av mars angreps ett finländskt företags e-postservrar så hårt att det under flera timmar var omöjligt att förmedla e-post till företag som använde dessa servrar. Attackeraren öppnade ett stort antal förbindelser i servrarna och lämnade förbindelserna öppna tills de löstes upp genom tidsövervakning.

Det är svårt att avvärja sådana attacker med begränsningar, eftersom attacktrafiken liknar vanlig trafik där förmedling av e-postmeddelanden är berättigad. Olika nät kan innehålla flera hundra eller flera tusen datorer som används för attacken. Det är svårt att använda finländska datorer för attack. Det beror på Kommunikationsverkets föreskrift 11/2004 M som anger att SMTP-trafiken från konsumentabonnemang endast är tillåten till internetoperatörens egen e-postserver.

Ny våg av internetbedrägeri

I mars upptäcktes igen en omfattande phishing-operation där man ville ta reda på bl.a. Nordea-bankkundernas användaridentifikationer och lösenord. Miljoner skräppostmeddelanden innehöll länkar till bluffsidor i flera olika länder. Denna gång lurades även finländska kunder att besöka sidorna.

De flesta av domännamn som användes på bluffsidorna hade registrerats i Hong Kong. Servrar hittades bl.a. i Estland, Rumänien, Bulgarien, Korea, Chile, Frankrike och Förenta Staterna. Nordea var inte ensam, utan totalt eller till och med flera hundra olika tjänster i samma servrar drabbades också av phishing.

13.4.2007

CERT-FI

Sättet för hur sidorna har byggts tyder på att man har använt ett Rock Phish Kit-verktygspaket som innehåller färdiga inställningar för att skapa webbsidor som liknar genuina nätbankers sidor. Med hjälp av paketet går det snabbt att skapa ett stort antal sidor som sedan kan användas för att samla användaridentifikationer och lösenord.

Uppgifter lurade med spionprogram

Den nya generationen av skadliga program som stjälar information och avlyssnar datoranvändare kan sägas vara född i februari 2006 när antivirusbolaget F-Secure fick de första rapporterna om Haxdoor. CERT-FI tog emot rapporter om de första finländska offren i juli 2006. Sedan dess har skadliga program som heter BZub och Torpig också använts.

CERT-FI har fått veta om flera loggservrar som används för spionprogram. Information som stjäls från användare av infekterade datorer lagras i dessa loggservrar. Loggservrarna befinner sig praktiskt taget alltid utomlands - och mycket ofta i samma nät. För tillfället är det för tidigt att säga, om det ökade antalet rapporterade loggservrar beror på att spionprogram blir allmänna eller att de som övervakar läget av skadliga program upptäcker sådana situationer bättre än tidigare.

Enligt CERT-FI:s iakttagelser är användare av finländska tjänster inte något huvudföremål för bedrägeri eller spionprogram, men verktygsprogram som används för att skapa phishing-sidor och skadliga program känner redan till finländska tjänster också. Det tycks vara så att när skadliga program utvecklas, så kan också mindre och lokala elektroniska tjänster för uträttande av ärenden bli utsatta för avlyssning.

Sårbarheter i programvaror för arbetsstationer

I början av året hittades flera sårbarheter i programvaror som används på arbetsstationer. En del av sårbarheterna har ännu inte åtgärdats.

I slutet av mars offentliggjordes en Windows-sårbarhet som hänför sig till hantering av animerade markörer (musens pekare). Sårbarheten gällde flera Windows-versioner, även den nya Windows Vista, och det var lätt att utnyttja den genom en webbsida eller ett e-postmeddelande. Microsoft publicerade en korrigerings snabbare än normalt genast i början av april.

Sårbarheter även i programvaror för industrin

I början av mars offentliggjordes sårbarheter i SCADA-produkter som används inom industrin för att styra processer i fabriker och förmedla därtill relaterade mätuppgifter. SCADA-produkters säkerhet har traditionellt inte varit under särskild kontroll därför att de befinner sig i produktionsanläggningarnas slutna nät.

SCADA-produkter ställer stora krav på säkerheten i nät- och IT-miljön. Även vanliga störningar i nätet kan orsaka allvarliga fel. Informationssäkerhetskränkningar av SCADA-system har ökat under de senaste åren.

Enligt CERT-FI:s beräkning kunde de sårbarheter som offentliggjordes i mars bilda ett hot mot system som är ytterst viktiga för samhällets kritiska funktioner. Riktade meddelanden och analyser om sårbarheterna skickades till innehavare av sådana system.

Sårbarheterna hittades med hjälp av testmaterial som en självständig aktör hade skapat. Sannolikt upptäckts flera sårbarheter på motsvarande sätt i andra SCADA-system.

13.4.2007

CERT-FI

Sårbarhet i nätverksutrustningar ledde till trafikfiltrering

I Cisco IOS-operativsystemet som används för internet-routerutrustningar offentliggjordes den 25 januari en sårbarhet som blev utnyttjad innan alla utrustningar hade uppdaterats med korrigeringar. Det ledde till att en del av operatörerna började filtrera nättrafik för att förebygga attacker. För användare betydde det att användningen av vissa tjänster hindrades.

Kampanjer för publicering av sårbarheter fortsatte

Publicering av sårbarheterna började politiseras förra året, och denna trend har fortsatt. I januari offentliggjordes 30 nya sårbarheter för Apple-programvaror. Människorna bakom temamånaden "The Month of Apple Bugs" meddelade att syftet med kampanjen var att få Apple förhålla sig till sårbarheterna i sina produkter på ett mer ansvarsfullt sätt.

I mars offentliggjordes 44 PHP-sårbarheter. PHP är ett mycket använt programmeringsspråk i nätapplikationer. Även "The Month of PHP Bugs" var ett svar till programutvecklarnas sätt att hantera sårbarheter som upptäckts i dem.

Fel och störningar

Några allvarliga fel eller störningar förekom inte. På förmiddagen den 19 februari upptäcktes ett fel i TeliaSonera Finlands e-posttjänst för konsumenter och företag. Under cirka tre timmars tid kunde man inte läsa e-postmeddelanden och konsumentkunderna kunde inte heller skicka några meddelanden.

Framtidsutsikter

CERT-FI håller för sannolikt att användare av finländska tjänster i framtiden också blir utsatta för systematiska försök till missbruk. De verktygssamlingar som används för att skapa skadliga program och bluffsidor innehåller redan webbadresser, namn och andra ämnesord för finländska tjänster.

Många elektroniska tjänster har visat sig vara sårbara för blockeringsattacker och flera riktade attacker kan förekomma. Attackerna kan riktas mot www-servrar, e-postservrar eller namnservrar. Tjänsteleverantörerna borde vara beredda för eventuella fientliga attacker. Attackerna kan utföras med skadliga program som sprider sig och fungerar självständigt eller med botnät.

Det är sannolikt att kampanjerna för publicering av sårbarheter fortsätter och att programtillverkare blir sysselsatta med korrigering av sårbarheterna. Alla anmälda kampanjer har dock inte realiserats eller deras inverknings har varit små i ljuset av publicerad information.

13.4.2007

CERT-FI**Terminologi:**

Blockeringsattack = Attack vars syfte är att förhindra tjänstens normala funktion och användning.

Rotnamnservrar (root name servers) = De tretton namnservrar som utgör en utgångspunkt vid sökning av uppgifter om namntjänst. I det hierarkiska domännamnssystemet för internet är dessa namnservrar på toppen av hierarkin.

Botnät (Botnet) = Nätverk av angripna datorer och kommandoservrar som står i förbindelse med dem. Angripna datorer kan hanteras på distans och de kan användas för skräppost eller blockeringsattacker utan att användaren vet om det.

Resolver (resolver) = Namnservrar som en till internet ansluten dator använder för DNS-förfrågningar. Den som frågar får svaret från en resolverserver som sedan sköter DNS-förfrågningar i stället för denna.

Rekursiv DNS-förfrågning (recursive dns query) = DNS-förfrågning där en resolver reder upp uppgift om namntjänst i stället för att den frågande datorn direkt skall ta kontakt med den auktoritära namnservern för frågeobjektet.

Autoritär namnservrar (authoritative name server) = Namnservrar som upprätthåller domännamnsrelaterade uppgifter, t.ex. IP-adresser, uppgifter om styrning av e-post, osv.

SCADA (Supervisory Control And Data Acquisition) = System för övervakning, styrning och datainsamling inom industrin.

PHP = Programmeringsspråk som används för att skapa och bearbeta innehållet i webbsidor.

SMTP (Simple Mail Transfer Protocol) = Protokoll som används för sändning av e-postmeddelanden till e-postservern och för förmedling av meddelanden mellan e-postserverna.